U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

August 21, 2017

BY CM/ECF

The Honorable P. Kevin Castel
United States District Judge
Southern District of New York
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street
New York, NY 10007

Re: *United States v. Kevin Forbes*, 17 Cr. 259 (PKC)

Dear Judge Castel:

The defendant in the above-captioned case is scheduled to be sentenced on August 30, 2017 at 12:00 p.m. For the reasons set forth below, the Government believes that a sentence within the Guidelines range of 30 to 37 months' imprisonment would be sufficient, but not greater than necessary, to meet the purposes of sentencing.

I. Offense Conduct

As described in the Presentence Investigation Report ("PSR"), the Defendant Kevin Forbes is the Managing Director of OilandGasPeople.com, which operates an online job board in the oil and gas industry and solicits job-seekers to upload their resumes (PSR ¶ 10). Between January 2017 and February 2017, the defendant informed a confidential source (the "CS") that he had accessed and downloaded a large quantity of resumes, email addresses, and customer data from a competitor ("Victim-1"). (PSR ¶ 11). The defendant offered to sell the resumes and customer data to the CS for approximately $250,000. (PSR ¶ 13). On or about February 23, 2017, the CS and an undercover law enforcement agent (the "UC") met with the defendant at a hotel in New York, NY, where the defendant used a laptop computer to log into a virtual private network and access Victim-1's company database. During the meeting, the defendant demonstrated his ability to view information related to resumes, subscribers, and employees who had uploaded information to Victim-1's database, including the usernames and passwords for subscribers. (PSR ¶ 14). The defendant was arrested on February 24, 2017. (PSR ¶ 15).

The defendant was charged in a criminal information (the "Information") on May 1, 2017 with one count of accessing a protected computer without authorization. (PSR ¶ 1).

II. The Defendant's Plea and Applicable Guidelines Range

On May 1, 2017, the defendant pleaded guilty to Count One of the Information pursuant to a plea agreement. Pursuant to U.S.S.G. § 2B1.1(a)(2), the plea agreement stipulated that the base offense level was six. Pursuant to U.S.S.G. § 2B1.1(b)(1)(I), the plea agreement stipulated that a 14-level enhancement applied because the loss exceeded $550,000, but was less than $1,500,000. Pursuant to U.S.S.G. § 2B1.1(b)(10)(B), a two-level enhancement applied because a substantial part of the fraudulent scheme was committed from outside the United States. Assuming a three-level reduction due to the defendant's acceptance of responsibility pursuant to U.S.S.G. § 3E1.1, the plea agreement stipulated a total offense level of 19. The plea agreement also stipulated that the defendant had zero criminal history points, resulting in a Criminal History Category of I. This calculation resulted in a Guidelines range of 30 to 37 months' imprisonment.

In the PSR, prepared on January 9, 2017, the Probation Office conducted the same calculation and also concluded that the defendant's applicable Guidelines range was 30 to 37 months' imprisonment. (PSR ¶¶ 24-35, 82).

III. Discussion

A. Applicable Law

Although *United States* v. *Booker* held that the Guidelines are no longer mandatory, it also held that they remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. 543 U.S. 220, 264 (2005). As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range," which "should be the starting point and the initial benchmark." *Gall* v. *United States*, 552 U.S. 38, 49 (2007).

After that calculation, a sentencing judge must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant;" (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available;" (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants;" and (7) "the need to provide restitution to any victims," 18 U.S.C. § 3553(a)(1)-(7). *See Gall*, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant; and
(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. A Sentence Within the Guidelines Range is Reasonable in this Case.

The Government submits that a sentence within the Guidelines range is appropriate in order to reflect the seriousness of the defendant's conduct, promote respect for the law, and provide just punishment for the offense.

At the outset, a sentence within the Guidelines range is necessary to reflect the seriousness of the defendant's conduct. Without any authorization whatsoever, the defendant accessed Victim-1's database and downloaded hundreds of thousands of subscriber resumes, intending to invite these subscribers to join OilandGasPeople.com. To cover his tracks, the defendant used a virtual private network so that Victim-1 would not be able to identify the defendant based on his Internet Protocol address. Additionally, the defendant hired contractors in India to download the resumes on an automated basis, allowing the defendant to download over 450,000 resumes undetected by Victim-1.[1] At the time when the FBI learned of the defendant's conduct, Victim-1 had still not yet identified the holes in its security infrastructure. As a result, Victim-1 spent hundreds of thousands of dollars in response, remediation, and investigation costs to identify and fix the vulnerability that the defendant had exploited. *See* U.S.S.G. § 2B1.1 n.3(A)(v)(III) (explaining that loss amount in offenses under 18 U.S.C. § 1030 includes costs of responding to an offense, conducting a damage assessment, and restoring the data).

Beyond that, the defendant possessed without authorization a spreadsheet containing customer data from 800 of Victim-1's customers, including recruiters and employers that paid for access to Victim-1's database. The customer data contained the terms and lengths of Victim-1's contracts with its customers, allowing the defendant a significant advantage in poaching Victim-1's clients, especially if the defendant were to successfully incorporate over 450,000 resumes from Victim-1 into his own company's database. Finally, it is worth emphasizing here that the defendant's actions were not detected by Victim-1 until the FBI brought the network intrusion to their attention. If not for the assistance of the FBI and the CS, the defendant likely would have continued this criminal activity, completely undetected. At a time when businesses and government agencies in the United States are reporting network intrusions on a regular basis--especially from extraterritorial actors like the defendant and his contractors in India--the Government submits that a significant term of incarceration is necessary here to protect the public from further crimes by the defendant, promote respect for the law, and discourage the defendant and similarly-situated individuals from engaging in similar criminal conduct in the future.

---

[1] *See* Application for Search Warrant, attached hereto as Exhibit A, at ¶ 13(d) ("During the meeting, FORBES also appeared to indicate that he worked with contractors in India (the "Indian Contractors") who were assisting him with downloading data from Website-1 in an automated fashion. FORBES stated that he communicated with the Indian Contractors using an anonymous email account. FORBES also indicated that he recruited another individual to send payments to the Indian Contractors.").

V. Conclusion

For the reasons set forth above, the Government respectfully requests that the Court impose a sentence within the Guidelines range of 30 to 37 months' imprisonment, as such a sentence would be sufficient but not greater than necessary to serve the legitimate purposes of sentencing.

Respectfully submitted,

JOON H. KIM
Acting United States Attorney

By: /s/ Andrew K. Chan
Andrew K. Chan
Assistant United States Attorney
(212) 637-1072

cc: Clay Kaminsky, Esq.